Application Number 09/900,494
Responsive to Office Action mailed October 3, 2005

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Currently Amended): A load balancing acceleration device, comprising:

a processor, memory and communications interface;

a TCP communications manager capable of interacting with a plurality of client devices and server devices simultaneously via the communications interface;

a secure communications manager to negotiate a secure communication session with one of the client devices;

an encryption and decryption engine instructing the processor to decrypt data received via the secure communications session and direct the decrypted data to one of said server devices via a second communication session; and

a load balancing engine associating each of said client devices with a respective one of said server devices based on calculated processing loads of each said server devices,

wherein the decryption engine and the load balancing engine bypass an application layer of a network stack by decrypting the data from the secure communication sessions of the clients and outputting the decrypted data to the associated server devices without processing the data with the application layer of the network stack.

Claim 2 (Previously Presented): The device of claim 1 wherein the TCP communications manager provides an IP address of an enterprise to said secure communications manager, and each of said plurality of servers devices is associated with the enterprise.

Claim 3 (Previously Presented): The device of claim 2 wherein the secure communications manager negotiates a secure communication session with each of said plurality of client devices over an open network.

Claim 4 (Previously Presented): The device of claim 3 wherein the TCP communications manager negotiates a separate, open communications session with one of the plurality of servers devices associated with the enterprise for each secure communications session negotiated with the a client devices based on the associations of said client devices to said server devices by said load balancing engines.

Claim 5 (Currently Amended): The device of claim 1 wherein the encryption and decryption engine decrypts the data on a packet level by decrypting packet data received on the communications interface via the secure communications session to extract a secure record, decrypting application data from the secure record in the packet data, and outputting the decrypted application data from the secure record to the one of said server devices via the second communication session without processing the application data with ~~an~~ the application layer of the network ~~a TCP/IP~~ stack.

Claim 6 (Previously Presented): The device of claim 5 wherein the load-balancing engine selects the second communication session.

Claim 7 (Previously Presented): The device of claim 1 wherein the TCP communications manager responds to TCP communications negotiations directly for an enterprise.

Claim 8 (Previously Presented): The device of claim 1,

wherein the TCP communications manager receives packets from the client devices, and

wherein the TCP communications manager changes destination IP addresses for the packets to IP addresses for the server devices.

Claim 9 (Previously Presented): The device of claim 8,

wherein the TCP communications manager maintains TCP communication sessions with the server devices, and

wherein the secure communications manager negotiates a secure communication session for each TCP communications session.

Claim 10 (Original): The device of claim 9 wherein the secure communications manager responds to all secure communications with each client device.

Claim 11 (Previously Presented): The device of claim 9 wherein the secure communications manager changes a destination IP address for each packet to a server IP address.

Claim 12 (Currently Amended): A method for performing acceleration of data communications between a plurality of customer devices attempting to communicate with an enterprise having a plurality of servers, comprising:

providing an intermediate acceleration device enabled for secure communication with the customer devices, wherein the acceleration device has an IP address associated with the enterprise;

receiving with the acceleration device communications directed to the enterprise in a secure protocol from one of the customer devices;

decrypting data packets of the secure protocol with the acceleration device to provide decrypted packet data;

without processing the data packets with an application layer of a network stack, selecting with the acceleration device at least one of the plurality of servers in the enterprise based on a load calculation including processing sessions of other servers in the enterprise and associating the selected server with a communications session from the one of the clients; and

forwarding the decrypted packet data from the acceleration device to the selected server of the enterprise.

Claim 13 (Original): The method of claim 12 further including the steps of:

receiving application data from the selected server of the enterprise;

encrypting the application data received from the selected server; and

forwarding encrypted application data to the customer device.

Claim 14 (Previously Presented): The method of claim 12 wherein the step of receiving communications directed to the enterprise includes receiving with the device communications having a destination IP address of the enterprise.

Claim 15 (Previously Presented): The method of claim 12 further including the step of negotiating the secure protocol session with the customer device by responding as the enterprise to the customer devices.

Claim 16 (Previously Presented): The method of claim 12 further wherein the step of forwarding comprises:

modifying a destination IP address of data packets from an IP address associated with the enterprise IP to an IP address for the selected server.

Claim 17 (Previously Presented): The method of claim 12 wherein the step of forwarding comprises:

establishing an open communication session from the acceleration device to the selected server, and

mapping the decrypted packet data to the open communication session established with the selected server.

Claim 18 (Previously Presented): The method of claim 17 wherein the open communication session is established via a secure network.

Claim 19 (Previously Presented): The method of claim 12 wherein the step of receiving comprises:

receiving encrypted data having a length greater than a TCP segment carrying said data; and

wherein said step of decrypting comprises:

buffering the encrypted data in a memory buffer in the acceleration device, the buffer having a length equivalent to the block cipher size necessary to perform the cipher; and

decrypting the buffered segment of the received encrypted data to provide decrypted application data.

Claim 20 (Currently Amended): The method of claim 19 further including the step of authenticating the data on receipt of a final TCP segment on a packet level without processing the application data with the ~~an~~ application layer of the network ~~a TCP/IP~~ stack.

Claim 21 (Original): The method of claim 19 further including the step of generating an alert if said step of authenticating results in a failure.

Claim 22 (Previously Presented): The device of claim 1, wherein the device comprises a network router.

Claim 23 (Currently Amended): The method of claim 12, wherein decrypting data packets comprises decrypting the data packets at a packet level of the network ~~a TCP/IP~~ stack.

Claim 24 (Currently Amended): The method of claim 12, wherein decrypting data packets comprises:

decrypting the data packets to extract a secure record,

decrypting application data from the secure record, and

authenticating the application data without processing the application data with ~~an~~ the application layer of the network ~~a TCP/IP~~ stack.

Claim 25 (Currently Amended): A system comprising:

a client device;

a plurality of server devices; and

an intermediate device coupled between the client devices and the server devices,

wherein the intermediate device intercepts a request from the client device for a secure communication session, and

wherein, in response to the request, the intermediate device establishes a secure communication session with the client device, selects one of the server devices based on resource loading experienced by the server devices without processing the request with an application layer of a network stack, and establishes a non-secure communication session with the selected server device.

Claim 26 (Previously Presented): The system of claim 25, wherein the intermediate device receives encrypted data from the client device via the secure communication session, decrypts the data and forwards the decrypted data to the selected server device via the non-secure communication session.

Claim 27 (Previously Presented): The system of claim 25, wherein the intermediate device receives unencrypted data from the selected server device via the non-secure communication session, encrypts the data and forwards the encrypted data to the client device via the secure communication session.

Claim 28 (Previously Presented): The system of claim 25, wherein the intermediate device comprises a network router.